# Data Security, zure enpresaren datu guztiak babesteko estrategia

Datuak enpresa baten aktiboen funtsezko atala dira. Bezeroen zorroak, jabetza intelektuala, merkataritza-ezagutza, produktuen katalogoak, enpresa-akordioak, I+G+B ekintzak… Informazio hori guztia funtsezkoa da erakunde baten funtzionamendurako, eta hardwarea, makineria, altzariak eta abar, bezalako ondasun ukigarriak baino garrantzitsuagoa izan daiteke. Horregatik, edozein enpresaren lehentasunetako bat Data Security edo datuen segurtasuna bermatzea da.

Data Security prozesuak aukera ematen dio erakunde bati bere informazioa babesteko baimenik gabeko sarbidearen, lapurretaren eta bizi-ziklo osoko datuen ustelkeriaren aurka. Aktibo kritiko horiek babestea funtsezkoa da enpresa baten funtzionamendurako, hainbat arrazoi direla medio:

· Ransomwareari edo enpresa baten informazioaren eta funtzionamenduaren bahiketari aurre egiten laguntzen du, adibidez, spam- edo phishing-iragazkien bidez.

· Mehatxuen eta giza akatsen datuak gordetzen laguntzen du, horiek baitira datuak urratzearen arrazoi nagusietako bat, firewalls bezalako tresnen bidez.

· Datu Pertsonalak Babesteari buruzko Legeria betetzea errazten du, eta hori ez betetzeak ekar ditzakeen zehapenak ez ezartzen saiatzen da.

· Enpresaren ospea babesten laguntzen du, besteak beste, sekretuen lapurreta eta jabetza intelektuala saihesten saiatzen delako.

Segurtasuna finkatzen eta gure enpresako informazioa babesten saiatzen diren tresna eta estrategia ugari daude. Mekanismo horiek funtsezkoak dira gure sarean erregistratzen den jarduera ezagutzeko eta jarduera susmagarriak detektatzeko, eta, hala badagokio, jarduera horiek ahalik eta eragin txikienarekin konpontzen lagunduko duen erantzun azkar eta irmoa emateko. Enpresa baten babes-mailetako bat **Datuen Babes Ingeniaritzak** eskaintzen du. Estrategia horren bidez, segurtasun-sare bat diseinatzen da. Horrek, hasiera batetik enpresa baten mehatxuetatik babesteko balio du eta mailakatu egiten da, erakundearen maila bakoitzak ahalik eta babes handiena izan dezan. Segurtasun-adar horrek hainbat neurri hartzen ditu segurtasun-proba gisa: kode-berrikuspenak eta segurtasun-arkitekturak eta mehatxuen aurrean sarea bloketatuta mantentzeko mehatxu-ereduak, besteak beste.

Beste maila batean, bereziki sentikorra edo konfidentziala den informazioa babesteko defentsa-ildoak aurkitzen dira. Horien arten garrantzitsuenetariko bat hodeian, memoria-gailu eramangarrietan edo posta elektronikoaren bidez bidalitako **dokumentuetan eta datu-baseetan enkriptatzea edo zifratzea** da. Tresna hori funtsezkoa da datuak babesteko, asko zailtzen baitu ziberkriminalek erabiltzea.

Babes-mekanismoetako bat suebakiak edo **firewalls**-ak dira. Tresna horiek segurtasun-ate gisa funtzionatzen dute konfiantza-sare baten eta segurua ez den beste baten artean, edukia iragaziz eta nahi ez den komunikazio potentzialaren bidez. Firewalls-ak hainbat gailu edo azpisareren barne-sistemetan jardun dezakete, bai eta enpresa baten sare lokalaren eta Interneten artean ere, sare-politiken eskakizunen arabera sarbideak baimendu edo ukatuz. Suebaki aukera desberdinak existitzen dira, enpresen beharren eta tamainaren arabera.

Firewall baten osagarri ezin hobea **Intrusioa Detektatzeko Sistemak** (IDS) dira, edozein intrusio detektatzeko erakunde baten sarean zabaltzen diren softwareak. Tresna horien artean daude ahultasunen eta fitxategien eskanerra, antimalwarea, honeypotak, etab. Intrusioak atzematen laguntzen dute. Gainera, zibersegurtasun-zentroetako erantzun-ekipoei edozein gorabehera jakinarazten zaie, hala nola BCSCren CERT -aren kasuan.

**Ahultasunen etengabeko analisia**

**Ahultasunak aztertzea** oinarrizko tresna da ziberdelinkuentziari eta datu-lapurretari aurre egiteko. Prozesu horren bidez, sare batean ezagutzen edo identifikatzen diren ahultasunak dituzten sistemak identifika daitezke, hala nola, exploitak, failak, segurtasun-bretxak, sarbide-puntu ez seguruak eta sistemaren konfigurazio-akatsak, haien eragina ebaluatzeko eta haiei aurre egiteko neurriak ezartzeko. BCSCren webgunean atal berezi bat dugu ahultasun horien berri emateko.

Irtenbide horietako bakar batek ere ezin dio eman zibersegurtasunaren arloko erakunde bati babes-mailarik handiena. Agertoki hori egin ahal izateko, enpresak eguneroko jardunean dituen mehatxu-mailetan oinarritutako **segurtasun-tresna edo -geruzak** erabili behar dira. Horietako bakoitzak zibersegurtasun-neurri batzuk ditu. Mehatxuak neutralizatzeko eta bere eremuan ireki daitezkeen ahultasunak eta arrailak murrizteko dira.

**Nola gorde zure datuak modu seguruan?**
Azkenik, zure enpresako datuak modu seguruan nola gorde behar diren zehaztu behar da. Hiru aukera daude:
· **Zuzeneko konexioaren biltegiratzea:** kanpoko disko gogorra izan daiteke, enpresa baten informazioa gordetzeko aukera ematen duena, datuak dituen gailura zuzenean konektatuta.
· **Sarean konektatutako biltegiratzea.** Hodei pribatua da, eta sare propiora konektatutako gailu bat da. Bertara tokiko edo kanpoko erabiltzaile-kredentzialen bidez sar daiteke.

Ikusi dezakezunez, datuak edozein enpresatako aktiborik garrantzitsuenetariko bat dira, horregatik, BCSCn egunero egiten dugu lan datuak modu seguruan gordetzen laguntzen duten tresnak erakusteko.